ON THE RANKS OF IWASAWA MODULES OVER p-ADIC LIE EXTENSIONS

YOSHIHIRO OCHI AND OTMAR VENJAKOB

ABSTRACT. In this paper we study Iwasawa modules arising from Galois cohomology over general p-adic Lie extensions both in the local and global case. In particular we calculate their Λ-ranks. Then we apply the results to abelian varieties.

1. INTRODUCTION

The Iwasawa theory for an elliptic curve over a $\mathbb{Z}_p$-extension of a number field was begun by B. Mazur ([Ma], 1972). Some years later, M. Harris began the study of the Iwasawa theory of an elliptic curve over the $GL_2(\mathbb{Z}_p)$-extension of a number field ([Ha1], 1979). Let E be an elliptic curve over a number field K without complex multiplication over $\bar{K}$ and consider $K_\infty = K(E[p^\infty])$, the field obtained by adjoining all p-power division points $E[p^\infty]$ of $E(\bar{K})$. By Serre's theorem [Se2, IV 2.2], after fixing a $\mathbb{Z}_p$-basis of the Tate module $T_p E$, the Galois group $G = G(K_\infty/K)$ is identified with an open subgroup of $GL_2(\mathbb{Z}_p)$, so G is a p-adic analytic group of dimension 4. The aim of this paper is to study Iwasawa modules, i.e. modules over the completed group algebra of G

$$(1) \qquad \Lambda(G) := \varprojlim \mathbb{Z}_p[G/U],$$

where U runs over all normal open subgroups of G. While at the moment we restrict to GL_2-extensions, we should point out that most of our results are obtained for general p-adic analytic extensions K_∞ over K.

One of the important Iwasawa modules is the Selmer group defined as follows:

$$(2) \qquad \mathrm{Sel}(E/K_\infty)\{p\} := \ker(H^1(K_\infty, E[p^\infty]) \to \prod H^1(K_{\infty,v}, E)(p)).$$

Since the cohomology groups have a natural continuous G-action as well as an action of $\mathbb{Z}_p$, the Selmer group is a discrete $\Lambda(G)$-module. Let $S = S(K)$ be a finite set of places of K such that S contains all places above p and ∞ and all places where E has bad reduction. Denote by K_S the maximal S-unramified extension of K and write $G_S(K_\infty) = \mathrm{Gal}(K_S/K_\infty)$. Then the Selmer group is also given by the following exact sequence

$$(3) \qquad 0 \to \mathrm{Sel}(E/K_\infty)\{p\} \to H^1(G_S(K_\infty), E[p^\infty]) \to \varinjlim_{n} \bigoplus_{w \in S(K_n)} H^1(K_{n,w}, E)(p).$$

The vanishing of $H^2(G_S(K_\infty), E[p^\infty])$, which immediately follows from the theorem of Iwasawa on the weak Leopoldt conjecture ([NSW, 10.3.25]), will allow us to obtain an unconditional result on the $\Lambda(G)$-(co)rank of the middle term. Our main concern is with the (co)rank of the Selmer group over K_∞ and there is a basic conjecture on this rank (Conjecture 7.4, also [CH, Conjecture 2.4]), but at this moment we are unable to prove this conjecture but have only some inequalities (Propositions 5.1 and 7.3).

The theory has recently made progress ([CH], [Ho3], [OV], [Su], [Ve1]), in particular structure theorems of torsion modules recently obtained by O. Venjakob (the p-torsion part, [Ve1]), S. Howson (the central torsion part, [Ho3]) and by J. Coates-P. Schneider-R. Sujatha (the general part, [CSS]). In this paper we will calculate the ranks of some Iwasawa modules arising from cohomology groups and determine their torsion submodules (see Theorems 3.2, 4.1, 4.3 etc.). We will also calculate the projective dimensions of certain Selmer groups (see Proposition 5.2 and Theorem 7.5) under the basic conjecture on the rank of the Selmer group mentioned above. In section 4 we refine Greenberg's results on the structure of Galois cohomology groups in local $\mathbb{Z}_p$-extensions (Theorem 4.3).

Iwasawa's initial work studied certain Galois groups as Γ-modules, where Γ is a Galois group isomorphic to $\mathbb{Z}_p$ as a topological group. The section 4 of this paper extends this case to the cases of general p-adic Lie extensions, and with natural assumptions we prove analogous results as Iwasawa's. Some of the results in the section were obtained by Harris but ours are slightly more general and we hope that our proofs are more structural by using Poitou-Tate duality.

This article will end with applications to the case of abelian varieties which was our main motivation of this work.

We will make a full use of the diagram in [OV, Lemma 4.5] , and the language of homotopy theory of modules, which we will review in the next section. This is a quite different approach from Harris' one that uses the common descent diagram [Ma, p. 231] and an asymptotic formula ([Ha1, Theorem 1.10 and Lemma 3.4.1], but [Ha2, Theorem 1.10] is better), neither of which shall appear in this paper.

2. Prerequisites

Let K be a finite extension of $\mathbb{Q}$ and p an odd prime number. Let V be a p-adic Galois representation of G_K, which is unramified except a finite set of primes of K. For instance $V = V_p E := T_p E \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ where $T_p E$ denotes the Tate module. For such a V we can take a finite set S of places of K containing each prime above p and every archimedean place and every place whose inertia group acts nontrivially on V. $S_f(K)$ denotes a subset of $S(K)$ which consists of all finite places in $S(K)$ and $S_p(K)$ is $\{v \in S_f(K) : v \mid p\}$.

We say that an extension K_∞/K is a *p-adic Lie extension* if it is a Galois extension and the Galois group $\mathrm{Gal}(K_\infty/K)$ is a compact p-adic Lie group of positive dimension. If it is a pro-p Lie group, we say K_∞/K is a pro-p Lie extension. *Throughout this paper, whenever we consider a p-adic Lie extension K_∞ of a number field K, we always assume that K_∞ is contained in K_S for some $S = S(K)$ associated to V.* The GL_2-extension in the introduction and $\mathbb{Z}_p^r$-extensions are examples of p-adic Lie extensions.

Let us fix V of dimension $dim_{\mathbb{Q}_p} V = r$, take a Galois-invariant $\mathbb{Z}_p$-lattice T of V and put $A = V/T$. Let K_∞ be a p-adic Lie extension of K with Galois group $G = G(K_\infty/K)$ contained in Ω, where Ω denotes the maximal S-ramified p-extension of $K(A)$, and $K(A)$ denotes the extension of K defined by the kernel of the representation $\rho : G_K \to \mathrm{Aut}(T)$. Put $\mathcal{H} = G(\Omega/K_\infty)$ and $\mathcal{G} = G(\Omega/K)$. Then we have established the following ([OV, 4.5]):

Diagram 2.1.

$$
\begin{array}{ccc}
0 & & 0 \\
\uparrow & & \uparrow \\
J_{A,K_\infty} & = & J_{A,K_\infty} \\
\uparrow & & \uparrow
\end{array}
$$

$$
0 \longrightarrow H^2(\mathrm{G}_{\mathrm{S},\infty}, A)^\vee \longrightarrow (\mathcal{N}^{ab}(p)^{\#})_{\mathcal{H}} \longrightarrow \Lambda(G)^{rd} \longrightarrow Y_{A,K_\infty} \longrightarrow 0
$$

$$
\| \qquad\qquad \cong\uparrow \qquad\qquad \uparrow \qquad\qquad \uparrow
$$

$$
0 \longrightarrow H^2(\mathrm{G}_{\mathrm{S},\infty}, A)^\vee \longrightarrow (H^1(\mathcal{N}^{ab}(p), A)^{\mathcal{H}})^\vee \longrightarrow H^1(\mathcal{R}, A) \longrightarrow H^1(\mathrm{G}_{\mathrm{S},\infty}, A)^\vee \longrightarrow 0
$$

$$
\uparrow \qquad\qquad \uparrow
$$

$$
0 \qquad\qquad 0
$$

Furthermore, $\mathcal{N}^{ab}(p)^{\#}$ is a projective $\Lambda(\mathcal{G})$-module, hence $(\mathcal{N}^{ab}(p)^{\#})_{\mathcal{H}}$ a projective $\Lambda(G)$-module, and the latter module is isomorphic to $(\mathcal{N}^{ab}(p)_{\mathcal{H}})^{\#}$ if the action of $\mathcal{H}$ on A is trivial.

When K is a finite extension of $\mathbb{Q}_l$ (including the case $l = p$), we have a similar diagram for any p-adic Lie extension K_∞/K inside an algebraic closure Ω of K.

We will explain the notation as much as necessary for our applications.

(i) For a finitely generated $\Lambda(\mathcal{G})$-module M, we defined

$$
(4) \qquad\qquad M[A] = M^{\#} := \mathrm{Hom}_{\mathbb{Z}_p,cont}(M, A)^\vee = M \otimes_{\mathbb{Z}_p} A^\vee.
$$

We recall that $\Lambda[A]$ is a free Λ-module of rank r.

(ii) $X = X_{A,K_\infty} = H_1(\mathcal{H}, A^\vee)$.

(iii) $Y = Y_{A,K_\infty} = (I(\mathcal{G})^{\#})_{\mathcal{H}}$, which has projective dimension ≤ 1 if $H^2(G_S(K_\infty), A) = 0$ since $(\mathcal{N}^{ab}(p)^{\#})_{\mathcal{H}}$ is a projective $\Lambda(G)$-module.

(iv) $J = J_{A,K_\infty} = \ker((\Lambda(\mathcal{G})^{\#})_{\mathcal{H}} \to (A^\vee)_{\mathcal{H}})$, which has no nonzero torsion submodule.

(v) $d = \dim_{\mathbb{F}_p} H^1(\mathcal{G}, \mathbb{F}_p)$ ([NSW, 3.9.1]).

Next we recall the language of homotopy theory of modules. Three functors are defined on the homotopy (stable) category $Ho(\Lambda)$ of finitely generated Λ-modules, the two of them we will use here: the loop space functor Ω and the transpose functor D. The transpose functor satisfies $D^2 = 1$. When two finitely generated Λ-modules M and N are isomorphic in the category (homotopically isomorphic), we write $M \simeq N$.

There is the following important exact sequence:

$$
(5) \qquad\qquad 0 \to \mathrm{E}^1(DM) \to M \stackrel{\phi_M}{\to} M^{++} \to \mathrm{E}^2(DM) \to 0.
$$

A finitely generated Λ-module M is called *reflexive* if the map ϕ_M in the sequence (5) is an isomorphism. It is proven that if Λ has no zero divisors and M is any finitely generated Λ-module, the set of all torsion elements in M forms a Λ-submodule of M, and it is isomorphic to $\mathrm{E}^1(DM) =: tor_\Lambda(M)$. The following result of Jannsen ([Ja1, 2.6]) is of frequent use in the sequel. We simplify the statements for our purpose.

Proposition 2.2. *Let G be a p-adic Lie group of dimension $= cd_p(G) = n$ and M a finitely generated $\Lambda(G)$-module, which is finitely generated as a $\mathbb{Z}_p$-module of rank r.*

(1) *If M is finite and nonzero, then $E^i(M) = 0$ except $i \neq n+1$ and $E^{n+1}(M) \neq 0$.*

(2) *If M is a free $\mathbb{Z}_p$-module, then $E^i(M) = 0$ unless $i = n$ and $E^n(M)$ is a free $\mathbb{Z}_p$-module of rank r and there is an isomorphism $E^n(M)^\vee \cong M \otimes D_n^{(p)}$, where $D_n^{(p)}$ denotes the p-dualizing module of G ([NSW, p.149]).*

Further Notation and Convention: We follow the notations in the paper [OV]. However the assumption on the prime number p was unnecessarily too restrictive there. At least as long as abelian varieties are treated, the case $p = 2$ is OK too. In any case $p = 3$ has no problem. In general the "Assumption I" put in the next section will be enough for our applications. For more convenience of the reader, we put a list of the notations.

(1) For an abelian group A, $A[p^m] := \ker(A \overset{\times p^m}{\to} A)$ and $A[p^\infty] := \bigcup_{n \geq 0} A[p^n]$. $\mu_{p^\infty} = \mathbb{G}_m[p^\infty]$ where $\mathbb{G}_m$ denotes the multiplicative group scheme over $\bar{\mathbb{Q}}$.

(2) For a $\mathbb{Z}_p$-module N, $N^\vee = \mathrm{Hom}_{\mathbb{Z}_p, cont}(N, \mathbb{Q}_p / \mathbb{Z}_p)$, is the Pontryagin dual of N, and for a p-divisible $\mathbb{Z}_p$-module, $N^* = \varinjlim_i \mathrm{Hom}(_{p^i}N, \mu_{p^\infty}) = T(N)^\vee(1)$, where $T(N) = \mathrm{Hom}(\mathbb{Q}_p / \mathbb{Z}_p, N) = \varprojlim _{p^i} N$.

(3) By a Noetherian ring, we mean a left and right Noetherian ring (with a multiplicative unit). By $pd_\Lambda(M)$ we denote the projective dimension of M. The global dimension of Λ is denoted by $pd(\Lambda)$.

(4) Let G be a profinite group and H a closed subgroup of G. For a $\Lambda(H)$-module M, we define $\mathrm{Ind}_G^H M := M \widehat{\otimes}_{\Lambda(H)} \Lambda(G)$ (compact induction), where $\widehat{\otimes}$ denotes completed tensor product. Also $\mathrm{Coind}_H^G M := \mathrm{Hom}_{\Lambda(H)}(M, \Lambda(G))$.

(5) Let K be a field of characteristic 0. We write G_K for the absolute Galois group $G(\bar{K}/K)$. For a G_K-module A, we use the notation $A(K) := H^0(G(\bar{K}/K), A)$.

(6) Let Λ be a ring, and M a Λ-module. Then $\mathrm{E}^i(M) := \mathrm{Ext}^i_\Lambda(M, \Lambda)$, and in the case $i = 0$, we also write $M^+ := \mathrm{E}^0(M)$.

(7) Galois cohomology is always continuous one.

(8) The G-module $\mathbb{Q}_p / \mathbb{Z}_p$ denotes an abelian group $\mathbb{Q}_p / \mathbb{Z}_p$ on which G acts trivially.

(9) For a finitely generated abelian p-primary group A we denote by A_{div} the quotient of A by its maximal p-divisible subgroup.

3. THE GLOBAL CASE

Let us fix a prime number p, a number field K, V, T and $S = S(K)$ as in the previous section. For a p-adic Lie extension K_∞/K, we write $X_S = H^1(G_S(K_\infty), A)^\vee$ and $U_v = H^1(K_{\infty,v}, A)^\vee$.

Proposition 3.1. *For any p-adic Lie extension K_∞/K, X_S and $\bigoplus_{v \in S(K)} Ind_G^{G_v} U_v$ are finitely generated over $\Lambda(G)$.*

Proof: This is immediate from the diagram. Firstly Y is finitely generated since there is a surjective morphism from a free Λ-module of finite rank. As Λ is Noetherian, X_S is also finitely generated. In the same way U_v is finitely generated over $\Lambda(G_v)$ and hence there is a surjective map $\Lambda(G_v)^k \to U_v$. Therefore there is also a surjective map

$\Lambda(G)^k = \Lambda(G) \otimes_{\Lambda(G_v)} \Lambda(G_v)^k \to \Lambda(G) \otimes_{\Lambda(G_v)} U_v$. It should be now obvious that the $\Lambda(G)$-module $\bigoplus_{v \in S(K)} \mathrm{Ind}_G^{G_v} U_v = \bigoplus_{v \in S(K)} (\Lambda(G) \otimes_{\Lambda(G_v)} U_v)$ is finitely generated over $\Lambda(G)$. $\qquad\square$

Let us recall the fact that if G is any pro-p group and has no element of order p, then $\Lambda(G)$ has no divisors of zero (see [DSMS]). It follows that $\Lambda(G)$ has a unique quotient field $Q(\Lambda)$ (division ring). For any finitely generated module M over such a $\Lambda(G)$, we define the rank of M, denoted by $\mathrm{rk}_\Lambda(M)$, to be $\dim_{Q(\Lambda)}(M \otimes_\Lambda Q(\Lambda))$.

Now we make the following assumption, which we will have to assume at many places.

Assumption I: *The prime number p is odd or if $p = 2$, then all global fields considered are totally imaginary.*

The following is a generalization of the one in the $\mathbb{Z}_p$-case ([Gr1, Prop. 3]) to general pro-p Lie extensions, assuming the above assumption.

Theorem 3.2. *Assume the Assumption I. Let K be a number field and A, S as above. For a pro-p Lie extension K_∞/K such that Λ is an integral domain, i.e., has no zero divisor, we have*

$$(6) \qquad rk_\Lambda(H^1(G_S(K_\infty), A)^\vee) - rk_\Lambda(H^2(G_S(K_\infty), A)^\vee) = r_2(K) \times r$$

where r is the $\mathbb{Z}_p$-corank of A and $r_2(K)$ is the number of complex places of K.

Proof: By [Ja1, 5.4],

$$(7) \qquad (\mathcal{N}^{ab}(p))_\mathcal{H} \cong \bigoplus_{v \in S'_\infty(K)} \mathrm{Ind}_G^{G_v} \mathbb{Z}_p \bigoplus \Lambda(G)^{d - r'_1 - r_2 - 1}$$

where $S'_\infty(K)$ is the set of real places of K which ramify in K_∞ and $r'_1 = \#S'_\infty(K)$. Since $\mathcal{G}$ is a pro-p group, $\Lambda(\mathcal{G})$ is a local ring and any projective module is free. Hence $N^{ab}(p)$ is a free $\Lambda(\mathcal{G})$-module: $N^{ab}(p) \cong \Lambda(\mathcal{G})^s$ for some s. Then $(N^{ab}(p)[A])_\mathcal{H} \cong (\Lambda(\mathcal{G})^s[A])_\mathcal{H} = \Lambda(G)^{rs} = (N^{ab}(p))_\mathcal{H}[A]$. Hence from the isomorphism (7), with the Assumption I, $s = d - r_2 - 1$. From the Diagram 2.1, the result follows. Note $\mathrm{rk}_\Lambda(J_{A,K_\infty}) = r$. $\qquad\square$

We should also like to consider the inverse limit version of these modules. We write

$$(8) \qquad H^i_{Iw}(K_\infty, \mathrm{T}_p A) := \varprojlim_{n,m} H^i(G_S(K_n), {}_{p^m}A).$$

Under the Assumption I, $H^i_{Iw}(K_\infty, \mathrm{T}_p A) = 0$ for $i > 2$ since $cd_p(G_S(K_n)) \le 2$.

Theorem 3.3. *The Λ-modules $H^i_{Iw}(K_\infty, \mathrm{T}_p A)$ are finitely generated and*

$$(9) \qquad rk_\Lambda(H^i_{Iw}(K_\infty, \mathrm{T}_p A)) = rk_\Lambda(H^i(G_S(K_\infty), A)^\vee).$$

Proof: There is the following spectral sequence due to Jannsen ([Ja2]):

$$(10) \qquad \mathrm{E}_2^{p,q} = \mathrm{E}^p(H^q(G_S(K_\infty), A)^\vee) \Longrightarrow H^{p+q}_{Iw}(K_\infty, \mathrm{T}_p A).$$

This gives the following exact sequence:

$$(11) \qquad \mathrm{E}^1(A(K_\infty)^\vee) \to H^1_{Iw}(K_\infty, \mathrm{T}_p A) \to \mathrm{E}^0(H^1(G_S(K_\infty), A)^\vee) \to \mathrm{E}^2(A(K_\infty)^\vee)$$

But $\mathrm{E}^i(M)$ are all torsion modules for $i \ge 1$ and any finitely generated Λ-module M (cf. [OV]). Therefore we obtain

$$\mathrm{rk}_\Lambda(H^1(G_S(K_\infty), A)^\vee) = \mathrm{rk}_\Lambda(\mathrm{E}^0(H^1(G_S(K_\infty), A)^\vee)) = \mathrm{rk}_\Lambda(H^1_{Iw}(K_\infty, \mathrm{T}_p A)).$$

There is a filtration $E_2^2 \subset E_1^2 \subset E_0^2 = E^2$ such that $E^2 = E_0^2/E_1^2 \cong E^{0,2}$, $E_1^2/E_2^2 \cong E^{1,1}$ and $E_2^2 \cong E^{1,0}$. This shows that $\mathrm{rk}_\Lambda(H^2(G_S(K_\infty), A)^\vee) = \mathrm{rk}_\Lambda(H_{Iw}^2(K_\infty, \mathrm{T}_pA))$. It is clear that $H_{Iw}^i(K_\infty, \mathrm{T}_pA)$ are finitely generated over Λ. $\qquad\square$

Remark: The spectral sequence of Jannsen and Proposition 3.3 also holds for any ℓ-adic local field, hence so does Theorem 3.3 (see Theorem 4.1 below).

By Propositions 3.2 and 3.3, we have

$$(12) \qquad \mathrm{rk}_\Lambda(H_{Iw}^1(K_\infty, \mathrm{T}_pA)) - \mathrm{rk}_\Lambda(H_{Iw}^2(K_\infty, \mathrm{T}_pA)) = r_2(K) \times \mathbb{Z}_p\text{-corank}(A).$$

From Proposition 2.2 and the long exact sequence (11), if $dim(G(K_\infty/k)) \geq 2$, then $H_{Iw}^1(K_\infty, \mathrm{T}_pA)$ has no nonzero torsion submodule. But more can be said:

Proposition 3.4. *Let K be a number field, and K_∞/K a p-adic Lie extension such that $dim(G(K_\infty/K)) \geq 3$. Then $H_{Iw}^1(K_\infty, \mathrm{T}_pA)$ is reflexive.*

Proof: Put $X = H^1(G_S(K_\infty), A)^\vee$ and $\mathbf{H}^1 = H_{Iw}^1(K_\infty, \mathrm{T}_pA)$. Then from the sequence (11), Proposition 2.2 and the assumption, we have $\mathbf{H}^1 = X^+$. Hence the sequence (5) becomes

$$(13) \qquad 0 \to \mathrm{E}^1(DX) \to X \xrightarrow{\phi} (\mathbf{H}^1)^+ \to \mathrm{E}^2(DX) \to 0.$$

Put $M = \mathrm{Coker}(\phi)$. Then the exact sequence $0 \to M \to (\mathbf{H}^1)^+ \to \mathrm{E}^2(DX) \to 0$ yields $0 \to (\mathbf{H}^1)^{++} \to M^+ \to \mathrm{E}^1\mathrm{E}^2(DX)$. But $\mathrm{E}^1\mathrm{E}^2(DX) = 0$ according to [OV, 2.4.3.]. Therefore $(\mathbf{H}^1)^{++} = M^+$. Another sequence $0 \to \mathrm{E}^1(DX) \to X \to M \to 0$ shows $M^+ = X^+ = \mathbf{H}^1$. Hence $\mathbf{H}^1 = (\mathbf{H}^1)^{++}$. $\qquad\square$

Proposition 3.5. *Let K be a number field, and K_∞/K a p-adic Lie extension such that $dim(G(K_\infty/K)) \geq 2$ and the Iwasawa algebra Λ is an integral domain. Then*

$$(14) \qquad tor_\Lambda(H^1(G_S(K_\infty), A)^\vee) \cong \mathrm{E}^1(H_{Iw}^2(K_\infty, \mathrm{T}_pA)).$$

Proof: Since J has no torsion part (see Section 2), $tor_\Lambda(X) = tor_\Lambda(Y)$. But [OV, 4.10] says $DY \simeq H_{Iw}^2(K_\infty, \mathrm{T}_pA)$. Hence $\mathrm{E}^1(DY) = \mathrm{E}^1(H_{Iw}^2(K_\infty, \mathrm{T}_pA))$. $\qquad\square$

Because of the isomorphism (14), the structure of $H_{Iw}^2(K_\infty, \mathrm{T}_pA)$ is more interesting but nothing is known except that if $H^2(G_S(K_\infty), A) = 0$, it is torsion by Theorem 3.3. The structure of $H^i(G_S(K_\infty), A)^\vee$ in the $\mathbb{Z}_p$ case, for $i = 1, 2$, is known as follows. Let us prove those from the results above.

Proposition 3.6 ([Gr1])**.** *Let K_∞/K be a $\mathbb{Z}_p$-extension and p odd. Then*

  (1) $H^2(G_S(K_\infty), A)^\vee$ *is a free Λ-module.*
  (2) *If $H^2(G_S(K_\infty), A)^\vee = 0$, then $H^1(G_S(K_\infty), A)^\vee$ has no finite submodule.*

Proof: Since $(\mathcal{N}^{ab}(p)^{\#})_\mathcal{H}$ is free and $pd(\Lambda) = 2$ in this case, $H^2(G_S(K_\infty), A)^\vee$ must be a projective Λ-module, and hence a free Λ-module as Λ is a local ring. If $H^2(G_S(K_\infty), A)^\vee = 0$, then $pd_\Lambda(Y) \leq 1$, and hence it has no finite submodule ([NSW, 5.5.3, iv]), and therefore $X = H^1(G_S(K_\infty), A)^\vee$ has no finite submodule. $\qquad\square$

For general p-adic Lie extensions, the first statement of the above proposition may not be true in general, though in many interesting cases it is predicted to be zero (see below "Assumption II"). At least it is torsion-free and $H^2(G_S(K_\infty), A)^\vee \simeq \Omega^2 Y$. The second statement of the proposition has been extended to higher dimensional pro-p Lie extensions, by Greenberg and Nguyen-Quang-Do (see [Ng]) in the commutative cases, and by the second author in the noncommutative cases (see [Ve1, 3.0.3] or [OV, 4.6]).

4. Local Results

Throughout this section K denotes a finite extension of $\mathbb{Q}_\ell$. Let A be as above and K_∞/K a p-adic Lie extension. First let us calculate a rank. We must assume that $\Lambda = \Lambda(G)$ is an integral domain. We begin by noting that $H^2(K_\infty, A) = 0$, because G_L has p-cohomological dimension ≤ 1 for any infinite Galois extension L of K such that $G(L/K)$ contains an infinite pro-p subgroup ([NSW, 7.1.8.i]).

Theorem 4.1. *Let K_∞/K be a pro-p Lie extension and denote the $\mathbb{Z}_p$-corank of A by r. Then*

$$rk_\Lambda H^1(K_\infty, A)^\vee = \begin{cases} r[K:\mathbb{Q}_p] & \text{if } \ell = p \\ 0 & \text{otherwise} \end{cases}.$$

The proof is similar to the one of Proposition 3.2, which will use the structure of $\mathcal{N}^{ab}(p)_\mathcal{H}$ in the local case ([Ja1, 5.1.c] in the case $\ell = p$). In the case $\ell \neq p$, we have $\mathcal{N}^{ab}(p)_\mathcal{H} = \Lambda$ and $d = 2$ if K contains μ_p and $\mathcal{N}^{ab}(p)_\mathcal{H} = 0$ and $d = 1$ otherwise. For the calculation of $d = \dim_{\mathbb{F}_p} H^1(K, \mathbb{Z}/p\mathbb{Z})$ see [NSW, 7.3.9]. The proof of the structure of $\mathcal{N}^{ab}(p)_\mathcal{H}$ is the same as the one for the case $\ell = p$, ([Ja1] or [NSW, 7.4.1]). Let us dare to have proof here as it is rather interesting. Firstly we look at the exact sequence of Galois groups $1 \to \mathcal{N} \to \mathcal{R} \to G_{K_n} \to 1$ (see the diagram just before Lemma 4.5 in [OV]; here we take $\mathcal{H} = G(\Omega/K_n)$). The inflation-restriction homology sequence with this sequence is

$$H^2(K_n, \mathbb{Q}_p/\mathbb{Z}_p)^\vee \to H_1(\mathcal{N}, \mathbb{Z}_p)_{G_{K_n}} \to H_1(\mathcal{R}, \mathbb{Z}_p) \to H_1(K_n, \mathbb{Z}_p) \to 0.$$

But $H^2(K_n, \mathbb{Q}_p/\mathbb{Z}_p) = 0$ (use Tate's local duality). Hence we get

$$(15) \qquad 0 \to \mathcal{N}^{ab}(p)_{G_{K_n}} \to \mathcal{R}^{ab}(p) \to G_{K_n}^{ab}(p) \to 0.$$

In the Grothendieck group $K_0(\mathbb{Q}_p[G_n])$, where $G_n = \text{Gal}(K_n/K)$, we have

$$(16) \qquad [\mathcal{N}^{ab}(p)_{G_{K_n}} \otimes \mathbb{Q}_p] = [\mathcal{R}^{ab}(p) \otimes \mathbb{Q}_p] - [G_{K_n}^{ab}(p) \otimes \mathbb{Q}_p].$$

To calculate $[\mathcal{R}^{ab}(p) \otimes \mathbb{Q}_p]$, we use the following exact sequence ("Fox-Lyndon resolution", [OV, Section 4.1]):

$$(17) \qquad 0 \to \mathcal{R}^{ab}(p) \to \mathbb{Q}_p[G_n]^d \to \mathbb{Q}_p[G_n] \to \mathbb{Z}_p \to 0$$

This sequence implies

$$[\mathcal{R}^{ab}(p) \otimes \mathbb{Q}_p] = [\mathbb{Q}_p[G_n]^d] - [\mathbb{Q}_p[G_n]] + [\mathbb{Q}_p] = [\mathbb{Q}_p[G_n]^{d-1}] - [\mathbb{Q}_p].$$

By local class field theory,

$$(18) \qquad G_{K_n}^{ab}(p) \cong \varprojlim_m K_n^\times/(K_n^\times)^{p^m} \cong H^1(K_n, \mathbb{Z}_p(1)).$$

Since $\ell \neq p$, $[H^1(K_n, \mathbb{Z}_p(1)) \otimes \mathbb{Q}_p] = [\mathbb{Q}_p]$ ([NSW, 7.3.10]). In conclusion we have obtained $[\mathcal{N}^{ab}(p)_{G_{K_n}} \otimes \mathbb{Q}_p] = [\mathbb{Q}_p[G_n]^{d-1}]$. Since $\mathcal{N}^{ab}(p)_\mathcal{H}$ is a projective Λ-module, $\mathcal{N}^{ab}(p)_\mathcal{H} \simeq \Lambda^{d-1}$. By (5.6.10) in [NSW] we get the result as required. Now the structure of $\mathcal{N}^{ab}(p)_\mathcal{H}$ is determined in both cases $\ell = p$ and $\ell \neq p$, we obtain Theorem 4.1 in the same way as Theorem 3.2.

We now assume K_∞/K is a $\mathbb{Z}_p$-extension. In this case Greenberg has proved the following basic results on the structure of the cohomology group $H^1(K_\infty, A)^\vee$.

Proposition 4.2 ([Gr1])**.** *Let K_∞/K be a $\mathbb{Z}_p$-extension and $r = \mathbb{Z}_p$-corank of A. Put $m = r[K:\mathbb{Q}_p]$.*

(1) *Assume $\ell = p$. Then $H^1(K_\infty, A)^\vee \sim \Lambda^m \bigoplus T_p A^*(K_\infty)$, where $\sim$ means pseudo-isomorphism.*

(2) *Assume $\ell = p$. If $A^*(K_\infty)$ is finite, then $X = H^1(K_\infty, A)^\vee$ is isomorphic to a submodule of Λ^m of finite index. The quotient Λ^m/X is isomorphic to a submodule of $A^*(K_\infty)$.*

(3) *Assume $\ell = p$. If $A^*(K_\infty) = 0$, then $H^1(K_\infty, A)^\vee$ is a free Λ-module of rank m.*

(4) *Assume $\ell \neq p$. Then $H^1(K_\infty, A)^\vee \sim T_p A^*(K_\infty)$. If $A^*(K_\infty)$ is finite, then $H^1(K_\infty, A) = 0$.*

We shall extend this result to extensions the Galois group of which is the semidirect product of $\Gamma \cong \mathbb{Z}_p$ with a finite group of order prime to p. Moreover, we get canonical exact sequences instead of just pseudo-isomorphisms.

Theorem 4.3. *Let K_∞/K be a Galois extension with the Galois group $G \cong \Gamma \rtimes_\omega \Delta$, where $\Gamma \cong \mathbb{Z}_p$ and Δ is a finite group of order t prime to p, which acts on Γ via the character $\omega : \Delta \to \mathbb{Z}_p^*$. We write $\chi = \omega^{-1}$ for the inverse of the character (of G) which determines the action on the p-dualizing module of G and we set $X = H^1(K_\infty, A^*)^\vee \cong H^1_{Iw}(K_\infty, T_p A)$. Let r be the $\mathbb{Z}_p$-codimension of A^*.*

(1) *If $l = p$, then the $\Lambda(G)$-module X fits into the canonical exact sequence*

$$0 \to T_p A(K_\infty) \to X \to P \to N \to 0$$

where P is a projective $\Lambda(G)$-module of $rk_{\Lambda(\Gamma)} P = rt[K : \mathbb{Q}_p]$ and the finite module N is determined by the exact sequence

$$0 \to N \to A(K_\infty)_{div}(\chi) \to tor_{\mathbb{Z}_p}(A^*(K_\infty)^\vee).$$

Furthermore,

(a) *if $A(K_\infty)$ is finite, then $T_p A(K_\infty)(\chi) = 0$. If, in addition, $A^*(K_\infty)^\vee$ is $\mathbb{Z}_p$-free, then $N \cong A(K_\infty)$.*

(b) *if $A(K_\infty)^\vee$ is $\mathbb{Z}_p$-free, then $X \cong P \oplus T_p A(K_\infty)(\chi)$. In particular, X is projective, if $A(K_\infty) = 0$.*

(2) *If $l \neq p$, then the $\Lambda(G)$-module X is isomorphic to*

$$X \cong T_p A(K_\infty)(\chi).$$

Proof: Recall the basic sequence of homotopy theory of modules:

(19) $$0 \to \mathrm{E}^1(DX) \to X \to X^{++} \to \mathrm{E}^2(DX) \to 0.$$

By [OV, Lemma 4.10 ,Proposition 4.11], we have

$$\mathrm{E}^1(DY) = \mathrm{E}^1(A(K_\infty)^\vee) = \mathrm{T}_p A(K_\infty)(\chi),$$

where the last equality follows from Proposition 2.2 and the fact that $D_1^{(p)}(\Gamma) = \mathbb{Q}_p/\mathbb{Z}_p(\omega)$. Since J has no torsion, $\mathrm{E}^1(DX) = tor_\Lambda(X) = tor_\Lambda(Y) = \mathrm{E}^1(DY) = \mathrm{T}_p A(K_\infty)(\chi)$.

From the exact sequence

$$0 \to X \to Y \to J \to 0,$$

we get an exact sequence

$$\mathrm{E}^1(J) \to \mathrm{E}^1(X) \to \mathrm{E}^1(Y) \to \mathrm{E}^2(J) = 0,$$

since J has no nonzero finite submodule([Ja1, 3.1.d]). From the exact sequence

$$0 \to J \to \Lambda[A^*] \to A^*(K_\infty)^\vee \to 0,$$

we get $\mathrm{E}^1(J) = \mathrm{E}^2(A^*(K_\infty)^\vee) = A^*(K_\infty)_{div}(\chi)$. Hence we have obtained the exact sequence

$$A^*(k_\infty)_{div}(\chi) \xrightarrow{\phi} \mathrm{E}^1(Y) \to \mathrm{E}^1(X) \to 0.$$

Denote $C = \mathrm{Coker}(\phi)$ and decompose this sequence into

$$0 \to C \to \mathrm{E}^1(Y) \to \mathrm{E}^1(X) \to 0$$

and

$$\mathrm{E}^1(J) \xrightarrow{f} C \to 0.$$

From the first one, we get

$$\mathrm{E}^1(C) \to \mathrm{E}^2(DX) \to \mathrm{E}^2(DY) \to \mathrm{E}^2(C) \to 0,$$

while from the second one

$$0 \to \mathrm{E}^1(C) \to \mathrm{E}^1\mathrm{E}^1(J) = \mathrm{E}^1(\mathrm{E}^2(A^*(K_\infty)^\vee)) = 0,$$

since $\mathrm{E}^2(A^*(K_\infty)^\vee)$ is finite ([Ja1, 3.1 (d)], and Proposition 2.2). Hence $\mathrm{E}^1(C) = 0$ and $E^2(DX)$ is a submodule of $E^2(DY) = E^2(A(K_\infty))^\vee = A^*(K_\infty)_{div}(\chi)$ while it is easily seen that $E^2(C) \subseteq \mathrm{tor}_{\mathbb{Z}_p}(A^*(K_\infty)^\vee)$ holds.

The facts that $\mathrm{pd}(\Lambda) = 2$ and Λ is local imply that X^{++} is a projective Λ-module. Hence from all the things shown above, we obtain the following exact sequence

$$0 \to \mathrm{T}_p A(K_\infty) \to X \to P \to N \to 0$$

where N is a submodule of the finite module $A^*(K_\infty)_{div}(\chi)$.

As we have already calculated, the rank of X, $\mathrm{rk}_{\Lambda(\Gamma)}(X) = rt[K : \mathbb{Q}_p]$ if $\ell = p$ and 0 otherwise, and obviously $\mathrm{rk}(X) = \mathrm{rk}(X^{++})$. $\qquad \square$

This theorem gives another proof of the following

Corollary 4.4 ([Gr2, 2.3]). *Let V be a one-dimensional p-adic representation of G_K and $A = V/T$ with any G_K-invariant $\mathbb{Z}_p$-lattice T in V. Then the $\mathbb{Z}_p$-corank of $H^1(K, A)$ is $[K : \mathbb{Q}_p] + \delta$, where $\delta = 1$ if $A = \mathbb{Q}_p / \mathbb{Z}_p$ or $A = \mu_{p^\infty}$, and $\delta = 0$ otherwise.*

Proof: Let K_∞/K be the cyclotomic $\mathbb{Z}_p$-extension with the Galois group Γ. Suppose $A \neq \mu_{p^\infty}$. Since there is no proper submodule of $\mathbb{Q}_p / \mathbb{Z}_p$ of finite index, $A^*(K_\infty)$ is finite. Put $\mathbf{H}^1 = H^1_{Iw}(K_\infty, \mathrm{T}_p A^*)$. We have the following exact short sequence

$$(20) \qquad\qquad 0 \to \mathbf{H}^1 \to \Lambda^{[K:\mathbb{Q}_p]} \to N \to 0$$

with some finite submodule N. Taking Γ-homology, we know the $\mathbb{Z}_p$-rank of $\mathbf{H}^1_\Gamma$ is $[K : \mathbb{Q}_p]$. Hence by the local duality, the $\mathbb{Z}_p$-rank of $(H^1(K_\infty, A)^\vee)_\Gamma$ is also $[K : \mathbb{Q}_p]$. Next we look at the exact inflation-restriction sequence:

$$(21) \qquad\qquad 0 \to H^1(\Gamma, A(K_\infty)) \to H^1(K, A) \to H^1(K_\infty, A)^\Gamma \to 0.$$

Now assume moreover $A \neq \mathbb{Q}_p / \mathbb{Z}_p$. Then $H^1(\Gamma, A(K_\infty))$ is finite, hence the $\mathbb{Z}_p$-corank of $H^1(K, A)$ is $[K : \mathbb{Q}_p]$. If $A = \mathbb{Q}_p / \mathbb{Z}_p$, then the $\mathbb{Z}_p$-corank of $H^1(K, \mathbb{Q}_p / \mathbb{Z}_p)$ is $[K : \mathbb{Q}_p] + 1$.

Finally let us consider the case $A = \mu_{p^\infty}$. In this case we will get similarly an exact sequence

$$0 \to \mathbb{Z}_p \to \mathbf{H}^1 \xrightarrow{f} \Lambda^{[K:\mathbb{Q}_p]} \to W \to 0$$

with some finite W. Put $Z = \text{Coker}(f)$. Then $H_1(\Gamma, Z) = H_2(\Gamma, W)$ is finite, hence the $\mathbb{Z}_p$-rank of $\mathbf{H}_\Gamma^1 = [K : \mathbb{Q}_p] + 1$. Since $H^1(\Gamma, A(K_\infty))$ finite, we get the $\mathbb{Z}_p$-corank of $H^1(K, \mu_{p^\infty}) = [K : \mathbb{Q}_p] + 1$. □

In the higher dimensional case the results are not as fine as above but still we obtain the following

Proposition 4.5. *Let K_∞/K be an p-adic Lie extension with Galois group G, such that $\dim(G) \geq 2$. Then the following hold:*

(1) *If $p \neq l$, then $H^1(K_\infty, A)^\vee = 0$.*
(2) *If $p = l$, then $H^1(K_\infty, A)^\vee$ is a torsion-free $\Lambda(G)$-module, which is even reflexive in case $cd_p \geq 3$.*

The proof is completely analogous to that of theorem 4.3 using again 2.2 and [OV, 4.10,4.11], see also [OV, 5.4]. Note that in the case $p \neq l$ the Galois group $G_k(p) \cong \mathbb{Z}_p(1) \rtimes \mathbb{Z}_p$ of the maximal p-extension of any local field over $\mathbb{Q}_\ell$ does not have any proper quotient G of $\dim(G) \geq 2$.

5. Selmer Groups

Let K be a number field and V and T as in Section 2. The Bloch-Kato Selmer group $\text{Sel}^{BK}(K, A)$ is defined as follows ([BK]):

$$\text{Sel}^{BK}(K, V/T) := \ker(H^1(K, V/T) \to \prod \widetilde{H}^1(K_v, V/T).$$

here, the definition of $\widetilde{H}^1$ is the following:

$$\widetilde{H}^1(K_v, V/T) = H^1(K_v, V/T)/Im(H_f^1(K_v, V/T))$$

where $Im(H_f^1(K_v, V/T))$ is the image of $H_f^1(K_v, V)$ under the natural map $V \to V/T$ and $H_f^1(K_v, V)$ is defined as follows:

If v does not divide p, then

$$H_f^1(K_v, V) := \ker(H^1(K_v, V) \to \prod H^1(K_v^{nr}, V))$$

where K_v^{nr} denotes the maximal unramified extension of K_v;

If v divides p, then

$$H_f^1(K_v, V) := \ker(H^1(K_v, V) \to \prod H^1(K_v, V \otimes_{\mathbb{Q}_p} B_{crys}))$$

where B_{crys} is the period ring defined by Fontaine ([Fo]).

It is shown in [BK] that for $V_p(E)$, where E is an elliptic curve over K, $H_f^1(K_v, V) = E(K_v) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and $\text{Sel}^{BK}(K, V/T) = \text{Sel}^{BK}(K, E[p^\infty]) = \text{Sel}(E/K)\{p\}$.

On the other hand Greenberg has defined a Selmer group for V which satisfies the so-called Panchishkin condition ([Gr3]). Let us recall the definition: V is said to satisfy the Panchishkin condition at the place v if

- V is de Rham.
- There is an exact sequence of p-adic representations

(22) $$0 \to \hat{V} \to V \to \tilde{V} \to 0$$

where $\hat{V}$ and $\tilde{V}$ satisfy $\hat{V} \otimes \mathbb{C}_p \cong \bigoplus_{i>0} \mathbb{C}_p(i)^{\oplus k_i}$ and $\tilde{V} \otimes \mathbb{C}_p \cong \bigoplus_{i\leq 0} \mathbb{C}_p(i)^{\oplus k_i}$ as G_{K_v}-modules.

If V satisfies the Panchishkin condition, then it satisfies the ordinary condition in the sense of [Gr1]. For a p-adic representation satisfying the Panchishkin condition, the Selmer group is defined in the following way:

(23)
$$\mathrm{Sel}^{Gr}(K, A) := \ker(H^1(G_S(K), A) \xrightarrow{\phi} \prod_{v|p} H^1(K_v^{nr}, A/F_v^+ A) \oplus \prod_{v \nmid p, v \in S} H^1(K_v^{nr}, A)),$$

where $F_v^+ A$ is a submodule of A defined by $\hat{V}$ in the Panchishkin filtration ($F_v^+ A$ is the image of $\hat{V}$ in A under the natural map), and S is a finite set of primes of K satisfying the condition as before.

We have the following long exact sequence deduced from Poitou-Tate's global duality and Tate's local duality:

$$0 \to \mathrm{Sel}^{BK}(K, V/T) \to H^1(G_S(K), V/T) \to \bigoplus_{v \in S(K)} \widetilde{H}^1(K_v, V/T)$$
$$\xrightarrow{\psi} \mathrm{Sel}^{BK}(K, T^*)^\vee \to H^2(G_S(K), V/T).$$

Here $\mathrm{Sel}(K, T^*)$ is defined as follows: Put $B_v = Im H_f^1(K_v, V)$. Let C_v be the orthogonal complement of B_v under the perfect paring of Tate's duality theorem. Then we define the Selmer group $\mathrm{Sel}^{BK}(K, T^*)$ as follows:

(24)
$$\mathrm{Sel}^{BK}(K, T^*) := \ker(H^1(G_S(K), T^*) \to \bigoplus_{v \in S(K)} H^1(K_v, T^*)/C_v).$$

The map ψ in the long exact sequence is obtained as follows. Put $A = V/T$ as before. Let us make the following notation: Write for any $i \geq 0$

(25)
$$\mathrm{III}^i(G_S(K), A) := \ker(H^i(G_S(K), A) \to \bigoplus_S H^i(K_v, A)).$$

By Poitou-Tate global duality we have the following commutative diagram:

$$
\begin{array}{ccccc}
0 & \to & \mathrm{III}^1(G_S(K), A^*)^\vee & \cong \mathrm{III}^2(G_S(K), A) \to H^2(G_S(K), A) & \text{(global duality)} \\
 & & \uparrow & & \\
 & & H^1(G_S(K), A^*) & & \\
 & & \uparrow & & \\
 & & \bigoplus_S H^1(K_v, A^*)^\vee & \cong \bigoplus_S H^1(K_v, T) & \text{(local duality)} \\
 & & \cup & \cup & \\
 & & \bigoplus_S (H^1(K_v, A^*)/C_v)^\vee = & \bigoplus_S B_v & \text{(by perfect paring)}
\end{array}
$$

Hence we get the following diagram commutative, which gives the long exact sequence:

$$
\begin{array}{ccc}
0 & & 0 \\
\downarrow & & \downarrow \\
\bigoplus_S B_v & = \bigoplus_S (H^1(K_v, A^*)/C_v)^\vee & \\
\downarrow & & \downarrow \\
H^1(G_S(K), A) \to \bigoplus_S H^1(K_v, A) & \to & H^1(G_S(K), T^*)^\vee \to H^2(G_S(K), A) \\
\| \qquad\qquad \downarrow & & \downarrow \qquad\qquad \| \\
H^1(G_S(K), A) \to \bigoplus_S H^1(K_v, A)/B_v \to & \mathrm{Sel}^{BK}(K, T^*)^\vee & \to H^2(G_S(K), A) \\
\downarrow & & \downarrow \\
0 & & 0
\end{array}
$$

Over an infinite Galois extension K_∞ of K we define the Selmer groups $\mathrm{Sel}^{BK}(K_\infty, V/T)$ to be the direct limit of the Selmer group over each layer. The same with $\mathrm{Sel}^{Gr}(K_\infty, V/T)$. We have similar long exact sequences as above for $\mathrm{Sel}^{BK}(K_\infty, V/T)$, $\mathrm{Sel}^{Gr}(K, V/T)$, and $\mathrm{Sel}^{Gr}(K_\infty, V/T)$. The finitely generatedness of $H^1(G_S(K_\infty), V/T)^\vee$ implies the one of $\mathrm{Sel}^?(K_\infty, V/T)$ for $? = BK$ or Gr.

From now on we assume that V satisfies the Panchishkin condition, we consider the Greenberg's Selmer group $\mathrm{Sel}^{Gr}(K, V/T)$ and omit Gr from the notation. Note that $\mathrm{Sel}^{BK}(K, V/T)$ is a submodule of $\mathrm{Sel}^{Gr}(K, V/T)$. We also assume the following

Assumption II: $H^2(G_S(K_\infty), A) = 0$.

For instance if K_∞ contains the cyclotomic $\mathbb{Z}_p$-extension, then this is believed to hold ([Gr1, Conjecture 3]).

The structure of the Selmer group, in particular, in the case $V = V_p(E)$, has been studied in [OV], where E/K is an elliptic curve without complex multiplication and has good ordinary reduction at any prime over p. There are also interesting results in other different cases (cf. [Gr2] and [Pe]). The following is easy.

Proposition 5.1. *Assume the Assumptions I and II. Then we have inequalities*

$$
(26) \qquad r \cdot r_2(K) - \Sigma_{v \in S_p}[K_v : \mathbb{Q}_p] codim(F_v^+ V) \le rk_\Lambda(Sel(K_\infty, A)^\vee) \le r \cdot r_2(K)
$$

where r is the dimension of V.

Proof: By the Assumption II and Theorem 3.2, we have

$$
\mathrm{rk}_\Lambda(H^1(G_S(K_\infty), A)^\vee) = r \cdot r_2(K).
$$

Hence $\mathrm{rk}_\Lambda(\mathrm{Sel}(K_\infty, A)^\vee) \le r \cdot r_2(K)$. In the same way one calculates with the results above to obtain

$$
\mathrm{rk}_\Lambda(\bigoplus_S H^1(K_{\infty,v}, A/F_v^+ A)) = \Sigma_{v \in S_p}[K_v : \mathbb{Q}_p].
$$

Hence from the exact sequence we get the other inequality

$$
r \cdot r_2(K) - \Sigma_{v \in S_p}[K_v : \mathbb{Q}_p]\mathrm{codim}(F_v^+ V) \le \mathrm{rk}_\Lambda(\mathrm{Sel}(K_\infty, A)^\vee).
$$

$\square$

The proof of [OV, Proposition 5.3] was not given, so we shall give it here.

Proposition 5.2. *Suppose that $3 \leq cd_p(G) = dim(G)$ and $dim(G) > cd_p(G_v) = dim(G_v)$ and $dim(G_v) \geq 2$ for any $v \nmid p$, and assume the morphism ϕ in the sequence (23) is surjective and the Assumption II. Then if $A(K_\infty)^\vee$ has a nontrivial finite submodule, then $pd_\Lambda(Sel(K_\infty, A)^\vee) = dim(G) - 1$ and if $A(K_\infty)^\vee$ has no finite submodule, then $pd_\Lambda(Sel(K_\infty, A)^\vee) = dim(G) - 2$.*

Proof: In this proof we also determine the projective dimension of $X = H^1(G_S(K_\infty), A)^\vee$ under the same assumptions in the statement. Let M be a Λ-module such that it is a finitely generated $\mathbb{Z}_p$-module. Then if it has no finite submodule, then $pd_\Lambda(M) = dim(G)$, and if it has a nontrivial finite submodule, then $pd_\Lambda(M) = dim(G) + 1$. This follows from Proposition 2.2. Indeed putting $n = \dim(G) = cd_p(G)$. By Proposition 2.2, if it has no finite submodule, then $E^n(M) \neq 0$, hence $pd_\Lambda(M) \geq dim(G)$ and if it has a nontrivial finite submodule, then $E^{n+1}(M) \neq 0$ and $pd_\Lambda(M) \geq dim(G) + 1$. But in any case $pd_\Lambda(M) \leq dim(G) + 1$ ([Br, 4.1]).

Now we recall the well-known fact from homological algebra: Given an exact sequence $0 \to N \to M \to L \to 0$, then we have

(27) $$pd_\Lambda(M) \leq \max\{pd_\Lambda(N), pd_\Lambda(L)\}.$$

and if it is not equality, then $pd_\Lambda(N) = pd_\Lambda(L) - 1$. Now we show the claim in the case that $A(K_\infty)^\vee$ has no finite submodule. We have the exact sequence $0 \to J \to \Lambda(G)[A] \to A(K_\infty)^\vee \to 0$, and since $pd_\Lambda(\Lambda(G)[A]) = 0$, $pd_\Lambda(J) = n - 1$. Now let us look at another sequence $0 \to X \to Y \to J \to 0$. By the assumption II, it is known from the Diagram 2.1 that $pd_\Lambda(Y) \leq 1$. As $n - 1 \geq 2$ by another assumption, $pd_\Lambda(X) = n - 2$.

Repeat the same thing with $H^1(K_{v,\infty}, A)^\vee$. Then with the assumption $\dim(G) > \dim(G_v)$ we get $pd_\Lambda(X_v) < n - 2$. Since $dim(G_v) \geq 2$, if v does not divide p, then $H^1(K_{v,\infty}, A)^\vee = 0$. Hence

$$pd_\Lambda(\bigoplus_S \mathrm{Ind}_G^{G_v} H^1(K_{v,\infty}, A)^\vee) = \max \bigoplus_S pd_\Lambda(\mathrm{Ind}_G^{G_v} H^1(K_{v,\infty}, A)^\vee) < n - 2.$$

Now from the long exact sequence above in the beginning of this section and (27), we get $pd_\Lambda(\mathrm{Sel}(K_\infty, A)^\vee) = dim(G) - 2$.

The case that $A(K_\infty)^\vee$ contains a nontrivial finite submodule goes similarly. $\square$

6. Galois Groups as Iwasawa Modules

In this section we consider the "original" case of Iwasawa theory, i.e., the case $A = \mathbb{Q}_p/\mathbb{Z}_p$ with trivial Galois action. Let K be a global number field and S a finite set of places of K containing all primes above p and ∞. The dual of the cohomology groups are isomorphic to Galois groups as Λ-modules, that is, $\mathfrak{X} = \mathrm{Gal}(L/K_\infty) = \mathrm{Sel}(K_\infty, \mathbb{Q}_p/\mathbb{Z}_p)^\vee$ and $X = \mathrm{Gal}(M/K_\infty) = H^1(G_S(K_\infty), \mathbb{Q}_p/\mathbb{Z}_p)^\vee$, where M is the maximal abelian pro-p S-ramified extension of K_∞ and L is the maximal unramified extension of K_∞. We also consider the extension L', the subextension of L, in which all primes of K_∞ split completely. Write $\mathfrak{X}' = \mathrm{Gal}(L'/K_\infty)$. We assume K_∞/K is a pro-p Lie extension such that its associated Iwasawa algebra has no nonzero zero divisor. For the results in this section the following is crucial

Assumption III: *No finite place of $S_f(K)$ splits completely in K_∞.*

The groups of global and local units are very important: In the following L denotes any finite extension of K contained in K_∞.

(1) $E_\infty = \varprojlim_L E'(L)$, where $E'(L)$ is p-adic completion of units of L: $E'(L) = \mathcal{O}_L^\times \otimes \mathbb{Z}_p$.

(2) $E_{S,\infty} = \varprojlim_L E'_S(L)$, where $E'_S(L)$ is p-adic completion of S-units of L: $E'(L) = \mathcal{O}_L^\times \otimes \mathbb{Z}_p$.

(3) $U_{S,\infty} = \bigoplus_{v \in S} \mathrm{Ind}_G^{G_v} U'_v(L_v)$, where $U'_v((L)$ is p-adic completion of units of L_v.

(4) $A_{S,\infty} = \bigoplus_{v \in S} \mathrm{Ind}_G^{G_v} A_v(L_v)$, where $A_v(L_v) = \varprojlim L^\times / L^{\times p^n}$.

The basic diagram connecting these modules is the following ([NSW, 11.3.10]):

$$
\begin{array}{ccccccccccc}
0 & \longrightarrow & H^2(G_S(K_\infty), \mathbb{Q}_p/\mathbb{Z}_p)^\vee & \longrightarrow & E_{S,\infty} & \longrightarrow & A_{S,\infty} & \longrightarrow & X_S & \longrightarrow & \mathfrak{X}' & \longrightarrow & 0 \\
& & \| & & \uparrow & & \uparrow & & \| & & \uparrow \\
0 & \longrightarrow & H^2(G_S(K_\infty), \mathbb{Q}_p/\mathbb{Z}_p)^\vee & \longrightarrow & E_\infty & \longrightarrow & U_{S,\infty} & \longrightarrow & X_S & \longrightarrow & \mathfrak{X} & \longrightarrow & 0
\end{array}
$$

There is also the following exact sequence:

$$(28) \qquad 0 \to E_\infty \to E_{S,\infty} \to \bigoplus_{S_{un}} \mathrm{Ind}_G^{G_v} \mathbb{Z}_p \to \mathfrak{X} \to \mathfrak{X}' \to 0,$$

where $S_{un} := \{\nu \in S(k) \mid p^\infty \nmid f_\nu\}$ and $f_\nu = f(k_{\infty,\nu}/k_\nu)$ denotes the degree of the extension of the corresponding residue class fields.

Now by the Assumption III, $\bigoplus_S \mathrm{Ind}_G^{G_v} \mathbb{Z}_p$ is torsion, so $\mathfrak{X}'$ is torsion if and only if $\mathfrak{X}'$ is torsion.

The main result of this section is the following

Theorem 6.1. $\mathfrak{X}'$ and $\mathfrak{X}$ are torsion Λ-modules under the Assumption III.

Lemma 6.2. Under the Assumption III, $H^2(G_S(K_\infty), A) = 0$ if and only if $\mathrm{III}^1(G_S(K_\infty), A^*)^\vee$ is Λ-torsion.

Proof: By [OV, Proposition 4.10 (ii)], $H^2(G_S(K_\infty, A) = 0$ if and only if $Z_A(K_\infty)$ (see loc. cit. for the definition) is Λ-torsion. From Poitou-Tate's global duality, we have the following exact sequence

$$(29) \qquad 0 \to \mathrm{III}^1(G_S(K_\infty), A^*)^\vee \to Z_A(K_\infty) \to \bigoplus_S (A^*)^\vee \otimes_{\Lambda(G_v)} \Lambda(G).$$

By the Assumption III, $\bigoplus_S (A^*)^\vee \otimes_{\Lambda(G_v)} \Lambda(G)$ is Λ-torsion. Hence $Z_A(K_\infty)$ is Λ-torsion if and only if $\mathrm{III}^1(K_\infty, A^*)^\vee$ is Λ-torsion. $\qquad\square$

Lemma 6.3. Under the assumption III, $H^2(G_S(K_\infty), \mu_{p^\infty}) = 0$.

Proof: Under the Assumption III,

$$H^2(G_S(K_\infty), \mu_{p^\infty}) = \mathrm{III}^2(K_\infty, \mu_{p^\infty}) = \varinjlim \mathrm{III}^1(G_S(K_n), \mathbb{Z}/p^m\mathbb{Z})$$

$$= \varinjlim_{n,m} Cl_S(K_n)/p^m = \varinjlim_n Cl_S(K_n) \otimes_\mathbb{Z} \mathbb{Q}_p/\mathbb{Z}_p = 0$$

since $Cl_S(K_n)$ is finite for every n. $\qquad\square$

Proof of Theorem 6.1:

It is easy to see that $\mathfrak{X}' \cong \mathrm{III}^1(K_\infty, \mathbb{Q}_p / \mathbb{Z}_p)^\vee$. Hence from the two lemmas above, $\mathfrak{X}'$ is Λ-torsion under the assumption III. Hence so is $\mathfrak{X}$ since $\mathfrak{X}'$ is torsion if and only if $\mathfrak{X}'$ is torsion.

Remarks:

1. In the case of any $\mathbb{Z}_p$-extension, Iwasawa proved that $\mathfrak{X}$ is a finitely generated Λ-torsion module. This follows from our results immediately, as the Assumption III is satisfied if S_f is taken to be the set of all primes of K above p.

2. It was claimed in [Ha1] that for a pro-p Lie extension K_∞/K such that K contains μ_p, $\mathfrak{X}$ is torsion (Theorem 3.3). However, the proof in [Ha1] was incorrect (but Harris himself has given a correct proof recently in [Ha2]). Our proof is quite different, and was discovered independently.

Proposition 6.4. *Assume the Assumption III and $H^2(G_S(K_\infty), \mathbb{Q}_p / \mathbb{Z}_p) = 0$ (the weak Leopoldt conjecture). Then*

(1) $rk_\Lambda(X_S) = r_2(K)$.
(2) $rk_\Lambda(A_{S,\infty}) = rk_\Lambda(U_{S,\infty}) = [K : \mathbb{Q}]$.
(3) $rk_\Lambda(E_{S,\infty}) = rk_\Lambda(E_\infty) = [K : \mathbb{Q}] - r_2(K)$.

Proof: From the vanishing assumption and Proposition 3.2, we get $rk_\Lambda(X_S) = r_2(K)$. There is an exact sequence (compare the sequence (28)):

$$(30) \qquad 0 \to U_{S,\infty} \to A_{S,\infty} \to \bigoplus_{S_{un}} \mathrm{Ind}_G^{G_v} \mathbb{Z}_p \to 0.$$

Hence the Assumption III says $rk_\Lambda(A_{S,\infty}) = rk_\Lambda(U_{S,\infty})$. By Kummer theory,

$$A_v(K_\infty) = \varprojlim_i (\varprojlim_n K_i^\times / K_i^{\times p^n}) = \varprojlim_i (\varprojlim_n H^i(K_{v,i}, \mathbb{Z}_p(1))).$$

By Proposition 3.3,

$$rk_\Lambda(\varprojlim_n H^i(K_{v,i}, \mathbb{Z}_p(1))) = rk_\Lambda(H^1(K_\infty, \mu_{p^\infty})).$$

But by Lemma 6.3, $H^2(K_\infty, \mu_{p^\infty}) = 0$, hence by Proposition 4.1, consequently we have $rk_{\Lambda(G_v)}(A_v(K_{\infty,v})) = [K_v : \mathbb{Q}_p]$. Therefore we have $rk_{\Lambda(G)}(\Lambda(G) \otimes_{\Lambda(G_v)} A_v(K_{\infty,v})) = \#\{v \in S_p(K)\} \times [K_v : \mathbb{Q}_p] = [K : \mathbb{Q}]$.

As the sequence (28) shows, $rk_\Lambda(E_{S,\infty}) = rk_\Lambda(E_\infty)$ under the Assumption III. But by now we know the ranks of $\mathfrak{X}$, X_S, $U_{S,\infty}$ and $A_{S,\infty}$. Hence from the diagram above we get $rk_\Lambda(E_{S,\infty}) = rk_\Lambda(E_\infty) = [K : \mathbb{Q}] - r_2(K)$. $\qquad\square$

7. Abelian Varieties

Let X be an abelian variety defined over a finite extension K of $\mathbb{Q}$, and X' denote the dual abelian variety of X. Throughout this section we put $A = X[p^\infty]$ and $A^* = X'[p^\infty]$, and we consider the Selmer group $\mathrm{Sel}^{BK}(K_\infty, A) = \mathrm{Sel}(X/K_\infty)\{p\}$ over the field $K_\infty = K(X[p^\infty])$ and just write $\mathrm{Sel}(K_\infty, A)$ omitting BK from the notation. Fix a finite set S of places of K which contains all primes above p and ∞ and all the primes where A has bad reduction. For an infinite extension K_∞ of K, we have a long exact

sequence, which is very basic for the Iwasawa theory of an abelian variety:

$$0 \to \mathrm{Sel}(K_\infty, A) \to H^1(G_S(K_\infty), A) \to \bigoplus_{v \in S(K)} \mathrm{Coind}_{G_v}^G H^1(K_{\infty,v}, X)(p)$$

$$\to (\varprojlim \mathrm{Sel}(K_n, \mathrm{T}_p X'))^\vee \to H^2(G_S(K_\infty), A).$$

In the classical Iwasawa theory this sequence is considered over a $\mathbb{Z}_p$-extension of K. In particular, when X is an elliptic curve over $\mathbb{Q}$ and for the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, then the structure of all these Λ-modules has been determined due to the recent work of K. Kato ([Ka]). In our case we can calculate the ranks of these modules, except the one of the Selmer group, relatively more easily than in $\mathbb{Z}_p$-cases. One reason is the following

Proposition 7.1. *(cf. [OV, 4.7]) Let K_∞ be as above. Then $H^2(G_S(K_\infty), A) = 0$.*

Another is the work of Coates and Greenberg on the Kummer theory for Selmer groups ([CG]). *From now on we assume that X has good reduction at all primes above p.* Then according to [CG], $K_{v,\infty} = K_v(X[p^\infty])$ is a deeply ramified field ([CG] for the definition) where v divides p, since it contains $K_v(\mu_{p^\infty})$ by the Weil pairing. Then there is the following isomorphism:

$$(31) \qquad\qquad H^1(K_{v,\infty}, X)(p) \cong H^1(K_{v,\infty}, \widetilde{X}[p^\infty])$$

where $\widetilde{X}$ is mod-p reduction of X, which is an abelian variety over an extension of $\mathbb{F}_p$ by assumption. From these we obtain the following

Proposition 7.2. *Let K be a finite extension of $\mathbb{Q}_\ell$, X an abelian variety over K of dimension g, and $K_\infty = K(A)$. Assume that X has good reduction. Put $G = \mathrm{Gal}(K_\infty/K_0)$ and $\Lambda = \Lambda(G)$, where $K_0 = K(X[p])$. Let r be the p-rank of $\widetilde{X}$. First suppose $\ell = p$.*

(1) *The Λ-rank of $H^1(K_\infty, A)^\vee$ is $2g[K_0 : \mathbb{Q}_p]$.*
(2) *The Λ-rank of $H^1(K_\infty, X)(p)^\vee$ is $r[K_0 : \mathbb{Q}_p]$.*
(3) *The Λ-rank of $(X(K_\infty) \otimes \mathbb{Q}_p / \mathbb{Z}_p)^\vee$ is $(2g - r)[K_0 : \mathbb{Q}_p]$.*
(4) *Now suppose $\ell \neq p$. Then $H^1(K_\infty, A) = H^1(K_\infty, X)(p)$ is Λ-torsion.*

Proof: The first and second statements follow from Theorem 4.1 and the isomorphism (31). For 3, use the well-known exact sequence:

$$0 \to X(K_\infty) \otimes \mathbb{Q}_p / \mathbb{Z}_p \to H^1(K_\infty, A) \to H^1(K_\infty, X)(p) \to 0.$$

and the isomorphism (31). Note if $\ell \neq p$, $X(K_\infty) \otimes \mathbb{Q}_p / \mathbb{Z}_p = 0$. The last statement follows from Proposition 4.5.

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Remark: The reason why we take K_0 as the base field is that the Galois group $G = \mathrm{Gal}(K_\infty/K_0)$ is a uniform group ([DSMS]) and therefore $\Lambda(G)$ is an integral domain.

The results in the global situation are the following. First let us prepare the following notation (as above, r_v denotes the p-rank):

$$\alpha_v = r_v[K_{0,v} : \mathbb{Q}_p] \text{ for } v \in S_p;$$

$$\alpha_p = \Sigma_{v \in S_p} \alpha_v;$$

$$\beta_v = (g - r_v)[K_{0,v} : \mathbb{Q}_p] \text{ for } v \in S_p;$$

$$\beta_p = \Sigma_{v \in S_p} \beta_v.$$

Proposition 7.3. *Let K be a finite extension of $\mathbb{Q}$, X an abelian variety over K of dimension g, and $K_\infty = K(A)$. Put $G = Gal(K_\infty / K_0)$ and $\Lambda = \Lambda(G)$. Then*

(1) *The Λ-rank of $H^1(G_S(K_\infty), A)^\vee$ is $g[K_0 : \mathbb{Q}_p]$.*
(2) *$H^2_{Iw}(K_\infty, T_pX)$ is Λ-torsion. The rank of $H^1_{Iw}(K_\infty, T_pX)$ is also $g[K_0 : \mathbb{Q}]$, which is torsion-free.*
(3) *The Λ-rank of $\Lambda(G) \otimes_{\Lambda(G_v)} H^1(K_{\infty,v}, X)(p)^\vee$ is α_v for any $v \in S_p$.*
(4) *$rk_\Lambda(Sel(K_\infty, A)^\vee) - rk_\Lambda(\varprojlim Sel(K_n, T_pX'))^\vee = \beta_p$. In particular,*

$$rk_\Lambda(Sel(K_\infty, A)^\vee) \geq \Sigma_{v \in S_p}(g - r_v)[K_{0,v} : \mathbb{Q}_p].$$

Proof: The first statement is obtained by using Theorem 3.2 with Proposition 7.1. This time we use the long exact sequence which is in the beginning of this section. $H^2_{Iw}(K_\infty, T_pA)$ is Λ-torsion because of Proposition 7.1 and [OV, 4.10]. The rank of $H^1_{Iw}(K_\infty, T_pA)$ is $r_2(K_0)$ by Theorem 3.3 and 1. The third statement follows from Proposition 7.2. The last statement follows from the long exact sequence in the beginning of this section and Proposition 5.1. $\qquad\square$

The following is the fundamental conjecture on the Selmer group:

Conjecture 7.4.

$$rk_\Lambda(Sel(K_\infty, A)^\vee) = \Sigma_{v \in S_p}(g - r_v)[K_{0,v} : \mathbb{Q}_p].$$

This would follow if the similar conjectures due to Mazur (ordinary case) and Schneider in the cyclotomic $\mathbb{Z}_p$-case are proven for *any* finite extension of $\mathbb{Q}$ ([Sc2], also [CH, 2.4]). We end this paper with the projective dimension of the Selmer group of an elliptic curve without complex multiplication.

Theorem 7.5. *Assume E is an elliptic curve without complex multiplication, has good reduction at any prime over p, and that the above rank conjecture holds. Let K_∞ be $K(E[p^\infty])$. Then the projective dimension of $Sel(K_\infty, E[p^\infty])^\vee$ is 2.*

Proof: This follows from Proposition 5.2 and Serre's calculation of the dimension of the Galois groups (see [Se2] and [CH]) and a result in [ST], which says that there is no bad reduction of additive type over K_0, and hence $dim(G_v) = 2$ or 3 maybe except the case E has supersingular reduction at v. But this case may be excluded thanks to the isomorphism (31). Hence we can say G and G_v satisfy the condition in Proposition 5.2 ($dim(G) = 4$ and $4 > dim(G_v) \geq 2$ for any v). Proposition 7.3.4 shows that the Conjecture implies the surjection of the map ϕ in the sequence (23), because the Conjecture with the vanishing of $H^2(G_S(K_\infty), E[p^\infty])$ implies that $\varprojlim_n Sel(K_n, T_pE)$ is torsion. But $\bigoplus_{v \in S(K_0)} H^1(K_{\infty,v}, E[p^\infty])$ has no nontrivial torsion submodule by Proposition 4.5. Hence $\varprojlim_n Sel(K_n, T_pE) = 0$ and therefore ϕ is surjective. $\qquad\square$

References

[BK]   S. Bloch and K. Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift I, Prog. Math. 86, 333-400, 1990.

[Br]   A. Brumer *Pseudocompact algebras, profinite groups and class formations*, J. Algebra, 4, 442-470, 1966.

[Co]   J. Coates, *Fragments of the GL_2 Iwasawa theory of elliptic curve without complex multiplication*, in Arithmetic of Elliptic Curves, LNM 1716, Springer 1999.

[CG]   J. Coates and R. Greenberg, *Kummer theory of abelian varieties over local fields*, Invent. Math., 124 (1996), 129-174.

[CH]   J. Coates and S. Howson, *Euler characteristics and elliptic curves II*, Journal of the Mathematical Society of Japan, 53 (1) (2001), pp. 175-235.

[CSS]   J. Coates, P. Schneider and R. Sujatha, *Modules over Iwasawa algebras*, preprint, 2001.

[DSMS] J.D. Dixon, M.P.F. du Sautoy, A. Mann, D. Segal. Analytic Pro-p Groups, Cambridge Studies in Advanced Mathematics 61, Cambridge University Press, 2nd edition, 1999.

[Fo]   J.-M. Fontaine, *Sur certaines types de representations p-adiques du groupe de Galois d'un corps local; construction d'un anneau de Barsotti-Tate*, Annals of Mathematics, 115 (1982), 529-577.

[Gr1]   R. Greenberg, *Iwasawa theory for p-adic representations*, Advanced Studies in Pure Mathematics 17, Algebraic Number Theory-in honour of K. Iwasawa 97-137, 1989.

[Gr2]   R. Greenberg, *Iwasawa theory for elliptic curves*, in Arithmetic of Elliptic Curves, LNM 1716, Springer, 1999.

[Gr3]   R. Greenberg, *Iwasawa theory and p-adic deformation of motives*, Proceedings of Symposia in Pure Mathematics, Volume 55 (1994), Part 2, pp.193-223.

[Ha1]   M. Harris, *p-adic Representations arising from descent on abelian varieties*, Compositio Math., 39(1979), 177-245.

[Ha2]   M. Harris, *Correction to "p-adic Representations arising from descent on abelian varieties"* , Compositio Math., 121(2000), 105-108.

[Ho1]   S. Howson, *Iwasawa theory of Elliptic Curves for p-adic Lie extensions*, Ph.D. thesis, University of Cambridge, July 1998.

[Ho2]   S. Howson, *Euler Characteristic as Invariants of Iwasawa Modules*, preprint, 2001.

[Ho3]   S. Howson, *Structure of central torsion Iwasawa modules*, preprint, 2001.

[Iw]   K. Iwasawa, *On $\mathbb{Z}_\ell$-extensions of algebraic number fields*, Ann of Math., 98, 246-326, 1973.

[Ja1]   U. Jannsen, *Iwasawa modules up to isomorphism*, Advanced Studies in Pure Mathematics 17, Algebraic Number Theory-in honour of K. Iwasawa 171-207, 1989.

[Ja2]   U. Jannsen, *A spectral sequence for Iwasawa adjoints*, unpublished notes 1994.

[Ka]   K. Kato, *p-adic Hodge theory and values of zeta functions of modular froms*, to appear in Asterisque.

[La]   M. Lazard, *Groupes analytiques p-adiques*, Publ. Math. I. H. E. S., 26, 1965.

[Ma]   B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. math., 18 (1972), 183-226.

[Ng]   T. Nguyen-Quang-Do, *Formations de classes et modules d'Iwasawa,in:* Number Theory Noordwigerhout 1983, LNM 1068, Spinger 1984.

[NSW]   J. Neukirch, A. Schmidt, K. Wingberg, Cohomology of Number Fields, Springer 2000.

[Oc]   Y. Ochi, *Iwasawa modules via homotopy theory*, PhD thesis, University of Cambridge, 1999.

[OV]   Y. Ochi and O. Venjakob, *On the structure of Selmer groups over p-adic Lie extensions*, to appear in Journal of Algebraic Geometry.

[Pe]   B. Perrin-Riou, *Groupe de Selmer d'une courbe elliptique a multiplication complexe*, Compo. Math., vol. 43 (1981), 387-417.

[Sc1]   P. Schneider, *Iwasawa L-functions of varieties over algebraic number fields, a first approach*, Invent. Math. 71 (1983), 251-293.

[Sc2]   P. Schneider, *p-adic Height pairings II*, Invent. Math. 79 (1985), 329-374.

[Sc3]   P. Schneider, *Motivic Iwasawa theory*, Advanced Studies in Pure Mathematics 17, Algebraic Number Theory-in honour of K. Iwasawa pp.421-456, 1989.

[Se1]   J-P. Serre, Cohomologie Galoisienne, Lecture Notes in Math., 5, Springer 1965.

[Se2]   J-P. Serre, Abelian ℓ-adic Representations and Elliptic Curves, W. A. Benjamin. INC, 1968.

[ST]   J-P. Serre and J. Tate, *Good reduction of abelain varieties*, Ann. of Math., 88 pp. 492-517, (1968).

[Si]   J. Silverman, The Arithmetic of Ellpitic Curves, Springer 1986.

[Su]   R. Sujatha, *Euler-Poincare characteristics of p-adic Lie groups and arithmetic*, preprint, 2000.
[Ve1]   O. Venjakob, *Iwasawa Theory of p-adic Lie extensions*, Dissertation, University of Heidelberg, 2000.
[Ve2]   O. Venjakob, *On the structure theory of the Iwasawa algebra of a p-adic Lie group*, preprint.
[Ve3]   O. Venjakob, *On the Iwasawa theory of p-adic Lie extensions*, preprint.
[We]   C. Weibel, Introduction to Homological Algebra, Cambridge U.P., 1994.
[Wa]   L. C. Washington, Introduction to Cyclotomic Fields, Second Edition, Springer, 1997.

KOREA INSTITUTE FOR ADVANCED STUDY (KIAS), 207-43 CHEONGRYANGRI-DONG, DONGDAEMUN-GU, SEOUL 130-012, SOUTH KOREA

E-mail address: `ochi@kias.re.kr`

UNIVERSITÄT HEIDELBERG, MATHEMATISCHES INSTITUT, IM NEUENHEIMER FELD 288, 69120 HEIDELBERG, GERMANY.

E-mail address: `otmar@mathi.uni-heidelberg.de`

URL: `http://www.mathi.uni-heidelberg.de/~otmar/`